(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 03/081932 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/IB02/02045

(22) International Filing Date: 27 March 2002 (27.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TUULOS, Martti** [FI/FI]; Pilotinkatu 38, FIN-33900 Tampere (FI). **VARANKI, Kari-Matti** [FI/FI]; Vihnuskallionkatu 6, FIN-37150 Nokia (FI).

(74) Agents: **STYLE, Kelda, Camilla, Karen** et al.; Page White & Farrer, 54 Doughty Street, London WC1N 2LS (GB).

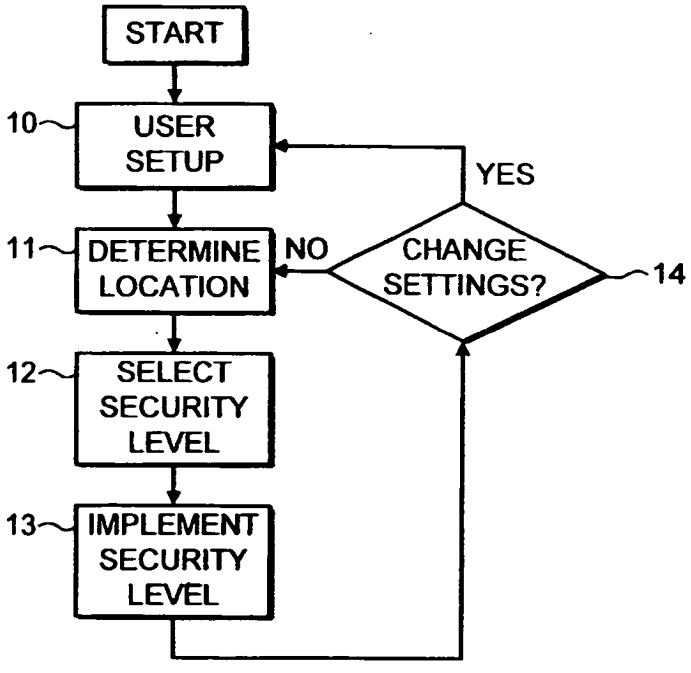
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MULTIPLE SECURITY LEVEL MOBILE TELECOMMUNICATIONS DEVICE, SYSTEM AND METHOD



(57) Abstract: A method and apparatus for implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network. The location of the mobile device is determined, and one of the first and second security levels is selected on the basis of that location. A security procedure is implemented within the mobile device on the basis of the selected security level.

WO 03/081932 A1

TITLE: MULTIPLE SECURITY LEVEL MOBILE TELECOMMUNICATIONS DEVICE, SYSTEM AND METHOD

FIELD OF INVENTION

The present invention relates to mobile telecommunications device security, and, more particularly, to implementing multiple security levels in such a device.

The invention has been developed primarily for use with mobile telephones and communication devices for use with third generation (UMTS) networks and will be described primarily with reference to this application. However, it will be appreciated that the invention has application under many other standards and protocols.

BACKGROUND OF INVENTION

Mobile telecommunications systems are known. One such example is the public land line mobile network (PLMN), of which cellular communications networks are an example. Another example is a mobile communication system that is based, at least partially, on use of communication satellites.

As the penetration rate of mobile phones into the population has increased, the incidence of theft, with or without violence, of such devices has increased. Whilst theft of current generation devices is costly and inconvenient to owners, the increase in available services and associated costs as networks are developed into the next generation mean that the potential for losses to users, network and insurers is higher than is presently the case. This is particularly the case where

mobile devices are able to access high cost services, or even capable of transferring cash value between bank accounts or various credit- or debit-based accounting systems.

One way to improve the security of mobile devices is to increase the amount of effort needed by the user to access services on the device. Many mobile handsets presently available, for example, can be configured to require a password to be input each time the device is to be used. Whilst this effectively prevents the device being used if it is stolen, entering, say, a personal identification number (PIN) or password each time a call is to be made is tedious for the user. In many cases, the user can disable this feature if it is known the phone is to be in safe environment, such as the user's home. However, changing the security status each time the user moves from a safe to an unsafe environment is also tedious. Moreover, if the user forgets to turn the security on, or if the device is stolen from the safe environment with the security disabled, there is nothing to stop the thief from accessing the services available via the phone.

In an unrelated aspect of mobile telecommunications, information regarding the geographical location of mobile devices can be ascertained for various purposes, such as accessing location-based services. For example, fairly accurate geographical location information can be obtained based on satellite-based GPS (Global Positioning System). More accurate location information can be obtained through differential GPS techniques.

Another possibility is to use a location service based on a cellular telecommunications system. In this approach, the cells or similar geographically limited radio access entities and associated controllers of the communication system are utilised in production of at least a rough estimate of the current location of the mobile user equipment. To improve the accuracy of the location information the communication system may be provided with specific location measurement units that provide more accurate data concerning the location of user equipment within the service area of the cellular system.

It is also possible to ascertain a geographical location when the mobile user equipment is located within the coverage area of a visited or "foreign" network. The visited network may be made capable of transmitting the location of the mobile user equipment back to the home network, e.g. to support services that are based on location information or for the purposes of routing and charging.

The location data may be processed in a specific location service entity that is implemented either within the cellular system or connected thereto. The location data may also be processed in the user equipment that is provided with appropriate processing capacity. The location service entity provided by the communication system may serve different clients via an appropriate interface.

The location information may be used for various purposes, such as for location of a mobile telephone that has made an emergency call, for locating vehicles or given mobile subscribers and so on.

An example of the provision of the location information by a PLMN is described in more detail 3rd Generation Partnership Project (3GPP) technical specifications, see e.g. 3GPP TS 23.271 version 4.2.0, titled "Functional stage 2 description of LCS", June 2001.

It is an object of the present invention to improve the ease with which multiple levels of security can be implemented in a mobile device configured for use within a communications network.

SUMMARY OF INVENTION

In a first aspect, the present invention provides a method of implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network, the method including the step of:

determining a location of the mobile device;

selecting one of the first and second security levels on the basis of the location; and

implementing a security procedure within the mobile device on the basis of the selected security level.

In a second aspect, the present invention provides a mobile telecommunications device for use within a telecommunications network, the mobile device having at least first and second security levels and being configured to:

determine its location;

select one of the first and second security levels on the basis of the location; and

implement a security procedure on the basis of the selected security level.

In a third aspect, the present invention provides a system for implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network, the system including:

location determination means for ascertaining a location of the mobile device;

means for selecting one of the first and second security levels on the basis of the location; and

means disposed within the mobile device for implementing a security procedure within the mobile device on the basis of the selected security level.

Preferably, the location is defined as an area.

In one form, wherein the location of the mobile device is determined by the telecommunications network. 23. Alternatively, the location is determined by the mobile device. In that case, the location of the mobile device is determined by:

receiving a signal at the mobile device;

ascertaining whether the signal is indicative of the device being within a relatively safe area; and

if the device is within a relatively safe are, implementing the relatively lower of the security levels within the mobile device.

Preferably, the location is used to generate a security level instruction, the security level instruction being sent to the mobile device for implementation.

In one embodiment, the location is defined in terms of a cell defined in the telecommunications network. In an

alternative embodiment, the location is defined in terms of proximity to one or more base stations within the telecommunications network.

In a preferred embodiment, the signal is a relatively short-range signal compared to call or data signals transmitted and received between the mobile device and the network.

Preferably, the signal includes unique data identifying a transmitter from which it is transmitted, thereby enabling the mobile device to ascertain whether it is in a location defined by proximity to the transmitter.

In one embodiment, the location is determined by reference to one or more external location providing signals. Preferably, the external location providing signals are GPS signals, the mobile device being configured to ascertain its location based on the GPS signals.

In a preferred form of the invention, the device is configured to receive input from a user, the input being indicative of a geographical range to be defined in relation to the location. The determination of the security level to be implemented is then based on the geographical range and the location. Preferably, the geographical range is defined in terms of a radius of operation with respect to the location.

In the preferred embodiment, the first security level is higher than the second security level. Preferably, the first security level requires more frequent input of identification or security data by a user than the second

security level, to prevent the mobile device entering a third security mode.

BRIEF DESCRIPTION OF DRAWINGS

A preferred embodiment of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a flowchart showing steps involved in implementing multiple level security levels in a mobile telecommunications device, in accordance with the invention.

Figure 2 is a schematic of a first embodiment of a mobile telecommunications device in use within a communications network, in accordance with the invention;

Figure 3 is a schematic of a second embodiment of a mobile telecommunications device for use within a communications network, in accordance with the invention; and

Figure 4 is a schematic of a third embodiment mobile telecommunications device in use within a communications network, in accordance with the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

It should be appreciated that even though the exemplifying telecommunications network shown and described in more detail uses the terminology of the third generation (3G) UMTS (Universal Mobile Telecommunications System) public land mobile network (PLMN), the proposed solution can be used in any system providing mobile communications for users and some kind

of location information service. Examples of other telecommunications systems include, without limiting to these, standards such as the GSM (Global System for Mobile communications) or various GSM based systems (such as GPRS: General Packet Radio Service), AMPS (American Mobile Phone System) or DAMPS (Digital AMPS), IMT 2000 (International Mobile Telecommunications system 2000), i-phone and so on.

Turning to Figure 2, there is shown an arrangement in which a cellular telecommunications system 20 provides coverage areas within cells 21 (for clarity, only a single cell is shown in its entirety). Each radio coverage area is served by a base station 22. It should be appreciated that one cell may include more than one base station, and that each base station apparatus or site may also serve or define more than one cell. The shape and size of the cells 21 depend on the particular implementation and can also vary from cell to cell within a single network. It should be appreciated that in some systems the base station may be referred to as Node B.

User equipment (UE) 23 is also shown, taking the form, in of a mobile. It shall be appreciated that typically a number of UEs will be in simultaneous communication with each base station, although for the sake of clarity only a single MS 23 is shown in this case. Each base station 22 is arranged to transmit signals to and receive signals from the MS 23 via a wireless interface, as is well understood by those skilled in the art. Likewise, the MS 23 is able to transmit signals to and receive signals from the base station 22.

The base station 22 is connected to an access network controller such as a radio network controller (RNC) of a UMTS terrestrial radio access network (UTRAN) within the core network 24. The radio network controller may be connected to appropriate core network entities of the cellular system, such as a MSC (mobile switching centre) and/or SGSN (serving general packet radio service support node), via a suitable interface arrangement. These, however, do not form an essential element of the invention and are thus not explained in any greater detail.

The location of the MS 23 may vary in time as the user equipment is free to move within the coverage area of a base station 22 and also from coverage to coverage area. Modern communication systems are capable of providing information regarding the geographical location of an MS within the coverage area of the network(s) within which they are operating. The geographical location may be defined on the basis of the position of the mobile station relative to the base station(s) of the mobile telecommunications network. The geographical location of the user equipment may also be defined, for example, in X and Y co-ordinates or in latitudes and longitudes. It is also possible to define the location of the base stations and/or mobile stations in vertical directions.

In Figure 2, location service (LCS) functionality of the communication system is provided by a Gateway Mobile Location Center (GMLC) entity 25. The GMLC gathers via appropriate interface means information concerning the location of the MS 23 from the cellular system.

The cellular system may be provided with various different means for processing information gathered from the cells and/or some other parameters and/or for computing by processor means appropriate calculations for determining and outputting the geographical location of the target user equipment.

The LCS 25 may thus be configured to provide, on request or periodically, the current or most recent geographic location of the target user equipment or, if the location fails, an error indication and optionally the reason for the failure. A more detailed description of a LCS entity that may be employed in the embodiments of the present invention can be found e.g. from the above referenced 3GPP technical specification No. 3GPP TS23.271.

It will be appreciated that the LCS server will usually be supported by other middleware such as one or more servers (not shown).

In use, the user of MS 23 is free to move around within the network 20, including from cell to cell 21. The user's location is periodically updated via the GMLC.

In the preferred form, the user of MS 23 is able to define locations that are considered relatively safe. So, for example, a user might define the areas adjacent his or her home and workplace as being relatively safe, and everywhere else as being relatively unsafe. The resolution of these areas is limited by the geographical resolution available from the GMLC. In some case, this resolution might simply be the cell 21 defined by the respective base stations closest to the user's home and workplace. In other case, the resolution can be smaller

than a single cell, base on, for example, triangulation between multiple base stations or handover data generated when the MS 23 is adjacent two or more cells.

The specific radius might also be set manually by a user, in metres, hundreds of metres or even kilometres from a particular area.

The MS 23 is also capable of operating in at least first and second security modes, the first security mode requiring higher security access than the second. The first security mode can, for example, require a longer password or PIN to be entered to access the MS 23 than the second security mode. In other embodiments, the first security mode can require a more frequent input of security data than the second mode. For example, in the first security mode, it might be necessary to input a PIN or password each time the phone is to be accessed, whilst the second security mode requires less frequent PIN or password access, or even no PIN or password input at all.

Periodically, the location of the MS 23 in relation to the network is established, and the data used to determine which security mode the MS 23 should be placed in.

In one embodiment, this determination takes place within the MS 23 itself, based on location data supplied from the GMLC via the base station 22. In this case, the mobile phone, upon determining that the MS 23 is within a relatively safe area automatically places itself into the second, lower security mode. Once the MS 23 is moved out of the relatively safe area, as determined with reference

to the location data, the security mode is automatically switched to the first, higher mode.

Turning to Figure 3, there is shown a second embodiment of the invention, in which the MS 23 is equipped with a Bluetooth™ receiver 30 designed to receive signals from a Bluetooth™ transmitter 31. The Bluetooth™ transmitter is a local, low power transmitter designed to transmit an identifying signal within a relatively short range. This could cover, for example, a home or office environment. The Bluetooth™ receiver in the MS 23 is configured to ascertain whether any signal received from a transmitter is a location signal that it recognises. In the event that the signal is recognised, the MS 23 determines that it is located in a relatively safe area and selects the second security mode. The presence of the signal is periodically determined. In the event it is no longer detected, the MS 23 selects the first, higher security mode on the basis that it is no longer in an area perceived as safe.

It will be appreciated that the selection of a Bluetooth™ local communication system is exemplary only, and that any suitable signal, of any scale, can be used to determine a safe area. For example, local radio station signals can be selected as enabling signals, such that the MS 23 is in the first security mode when the signal is present and in the second mode when the signal is absent.

Turning to Figure 4, there is shown yet another embodiment in which the location is determined by Global Positioning System (GPS) data. The operation of GPS is well known and so will not be described in detail here.

In general terms, by comparing time delays in signals from a number of different geosynchronous satellites, it is possible to compute the location of the MS 23 with considerable accuracy. In this case, the MS 23 is capable of determining its own location by means of an inbuilt GPS receiver 40 and then ascertaining which security mode it should enter. This can be done with reference to a look up table 41 of safe (or, less likely, unsafe) areas or locations. In the illustrated form, this table 41 is stored as part of the subscriber's profile data 42 stored within the network. Alternatively, a similar table can be stored in the MS 23 itself.

Although the invention has been described in relation to two security modes, it will be appreciated that it can be expanded to cover any number of security modes. For example, a low security mode can be defined for use in the home, a medium security for use in the workplace and high security elsewhere. Also, multiple different locations can share the same security setting.

It will also be understood that the security mode can be decided entirely within the network on the basis of the user's definitions of locations or areas, and the security mode selected automatically based on an instructions sent to the MS 23 from the network. For example, the network may define certain areas as dangerous for mobile phone theft, and transmit an instruction to all mobile devices within that area to enter a relatively high security mode if they have the capability. In other embodiments, the user can optionally configure the MS 23 to ignore such commands,

or to give a warning that the area is considered unsafe without actually entering a different security mode.

In the preferred form, the invention requires the user to periodically enter identification to ensure the MS 23 does not enter a locked mode that is relatively difficult to unlock.

The actual ways in which users authenticate themselves are not important to the operation of the invention. Whilst passwords and PINs have been described above, biometrics such as heart rate, fingerprint or retinal scanning or voice analysis can also be used to identify the user in one or more of the selectable security modes. In yet other embodiments, smart cards, swipe cards or other data bearing media can be used to unlock the MS23.

It will be appreciated that in yet other embodiments, allowing the MS 23 to go into sleep mode due to a failure of the user to undertake the required authentication steps can require network intervention to unlock the MS 23.

Although the invention has been described with reference to a specific examples, it will be appreciated that the invention can be embodied in many other forms.

CLAIMS

1. A method of implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network, the method including the step of:

determining a location of the mobile device;

selecting one of the first and second security levels on the basis of the location; and

implementing a security procedure within the mobile device on the basis of the selected security level.

2. A method according to claim 1, wherein the location is defined as an area.

3. A method according to claim 1 or 2, wherein the location of the mobile device is determined by the telecommunications network.

4. A method according to claim 3, wherein the location is used to generate a security level instruction, the security level instruction being sent to the mobile device for implementation.

5. A method according to any one of the preceding claims, wherein the location is defined in terms of a cell defined in the telecommunications network.

6. A method according to any one of claims 1 to 4, wherein the location is defined in terms of proximity to one or more base stations within the telecommunications network.

7. A method according to claim 1 or 2, wherein the location is determined by the mobile device.

8. A method according to claim 7, wherein the step of determining the location of the mobile device includes the steps of:

receiving a signal at the mobile device;

ascertaining whether the signal is indicative of the device being within a relatively safe area; and

if the device is within a relatively safe are, implementing the relatively lower of the security levels within the mobile device.

9. A method according to claim 8, wherein the signal is a relatively short-range signal compared to call or data signals transmitted and received between the mobile device and the network.

10. A method according to claim 8 or 9, wherein the signal includes unique data identifying a transmitter from which it is transmitted, thereby enabling the mobile device to ascertain whether it is in a location defined by proximity to the transmitter.

11. A method according to claim 7, wherein the location is determined by reference to one or more external location providing signals.

12. A method according to claim 11, wherein the external location providing signals are GPS signals, the mobile device being configured to ascertain its location based on the GPS signals.

13. A method according to any one of the preceding claims, further including the step of receiving, in the mobile device, input from a user, the input being indicative of a geographical range to be defined in relation to the location, the determination of the security level to be implemented being based on the geographical range and the location.

14. A method according to claim 13, wherein the geographical range is defined in terms of a radius of operation with respect to the location.

15. A method according to any one of the preceding claims, wherein the first security level is higher than the second security level.

16. A method according to claim 15, wherein the first security level requires more frequent input of identification or security data by a user than the second security level, to prevent the mobile device entering a higher security mode.

17. A mobile telecommunications device for use within a telecommunications network, the mobile device having at least first and second security levels and being configured to:

determine its location;

select one of the first and second security levels on the basis of the location; and

implement a security procedure on the basis of the selected security level.

18. A mobile telecommunications device according to claim 17, wherein the location is defined as an area.

19. A mobile telecommunications device according to claim 17 or 18, wherein the location of the mobile device is determined by the telecommunications network.

20. A mobile telecommunications device according to claim 19, wherein the location is used to generate a security level instruction, the security level instruction being sent to the mobile device for implementation.

21. A mobile telecommunications device according to any one of claims 17 to 20, wherein the location is defined in terms of a cell defined in the telecommunications network.

22. A mobile telecommunications device according to any one of claims 17 to 20, wherein the location is defined in terms of proximity to one or more base stations within the telecommunications network.

23. A mobile telecommunications device according to claim 17 or 18, wherein the location is determined by the mobile device.

24. A mobile telecommunications device according to claim 23, wherein the step of determining the location of the mobile device includes the steps of:

receiving a signal at the mobile device;

ascertaining whether the signal is indicative of the device being within a relatively safe area; and

if the device is within a relatively safe are, implementing the relatively lower of the security levels within the mobile device.

25. A mobile telecommunications device according to claim 24, wherein the signal is a relatively short-range signal compared to call or data signals transmitted and received between the mobile device and the network.

26. A mobile telecommunications device according to claim 24 or 25, wherein the signal includes unique data identifying a transmitter from which it is transmitted, thereby enabling the mobile device to ascertain whether it is in a location defined by proximity to the transmitter.

27. A mobile telecommunications device according to claim 23, wherein the location is determined by reference to one or more external location providing signals.

28. A mobile telecommunications device according to claim 27, wherein the external location providing signals are GPS signals, the mobile device being configured to ascertain its location based on the GPS signals.

29. A mobile telecommunications device according to any one of claims 17 to 28, further including the step of receiving, in the mobile device, input from a user, the input being indicative of a geographical range to be defined in relation to the location, the determination of the security level to be implemented being based on the geographical range and the location.

30. A mobile telecommunications device according to claim 29, wherein the geographical range is defined in terms of a radius of operation with respect to the location.

31. A mobile telecommunications device according to any one of claim 17 to 30, wherein the first security level is higher than the second security level.

32. A mobile telecommunications device according to claim 31, wherein the first security level requires more frequent input of identification or security data by a user than the second security level, to prevent the mobile device entering a third security mode.

33. A system for implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network, the system including:

location determination means for ascertaining a location of the mobile device;

means for selecting one of the first and second security levels on the basis of the location; and

means disposed within the mobile device for implementing a security procedure within the mobile device on the basis of the selected security level.

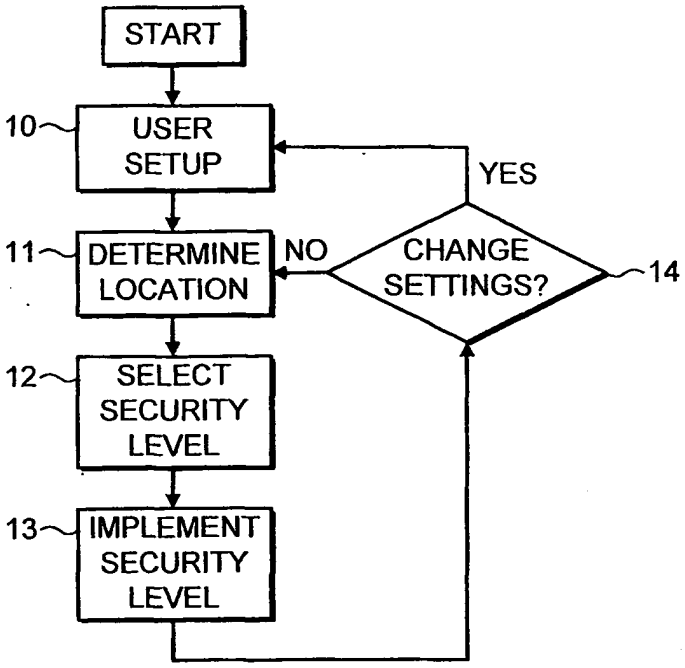

START
10
USER SETUP
YES
11
DETERMINE LOCATION
NO
CHANGE SETTINGS?
14
12
SELECT SECURITY LEVEL
13
IMPLEMENT SECURITY LEVEL

FIG. 1

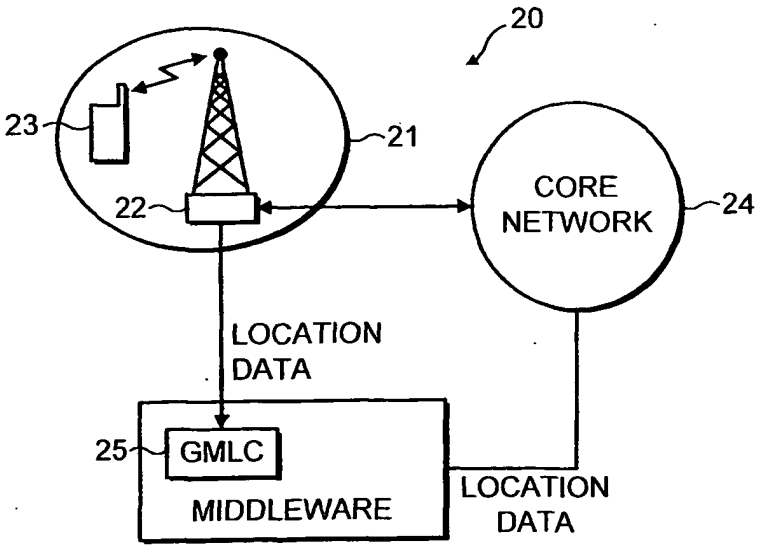

20
23
21
22
CORE NETWORK
24
LOCATION DATA
25
GMLC
MIDDLEWARE
LOCATION DATA

FIG. 2

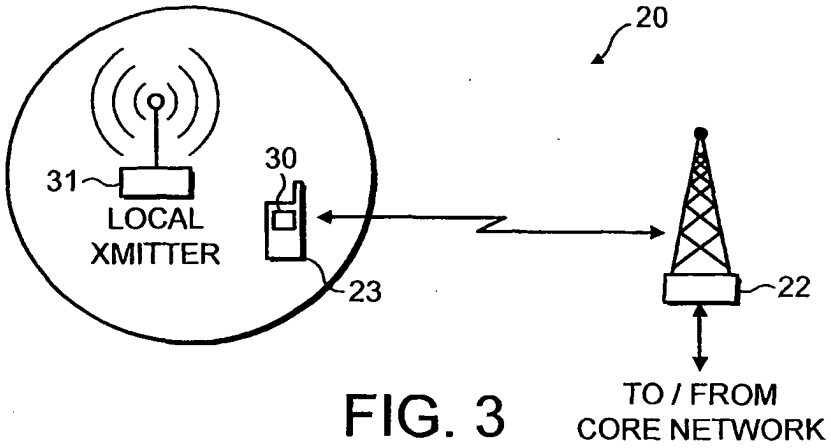

20
31
LOCAL
XMITTER
30
23
22
TO / FROM
CORE NETWORK

FIG. 3

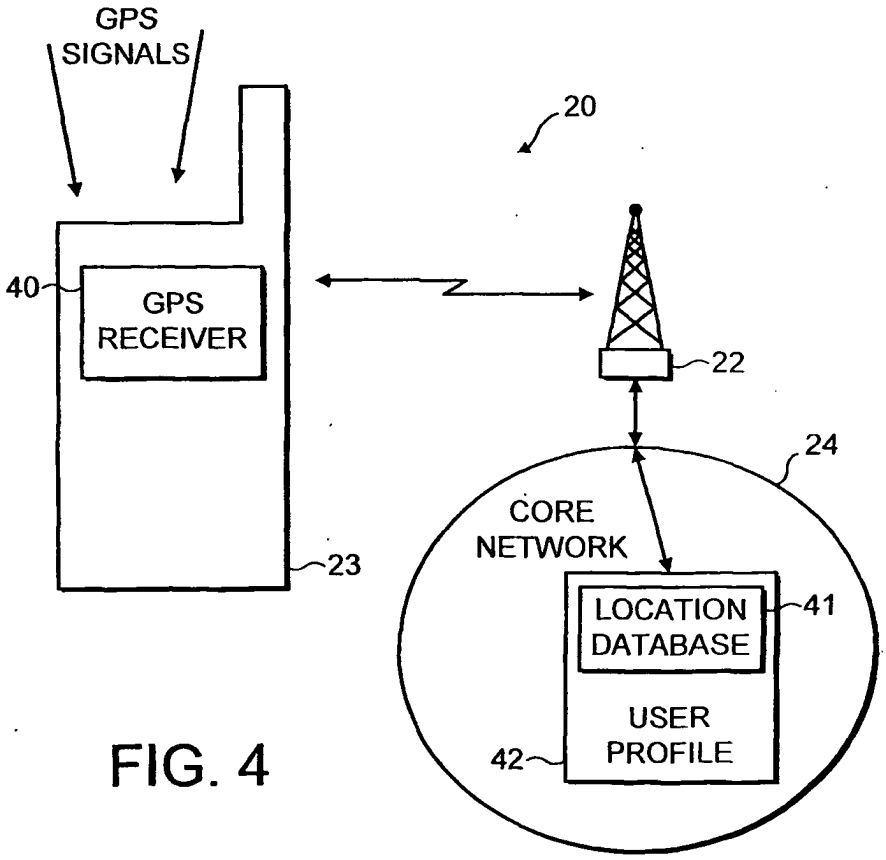

GPS
SIGNALS
20
40
GPS
RECEIVER
22
24
CORE
NETWORK
23
LOCATION
DATABASE
41
USER
PROFILE
42

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB 02/02045

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 150 531 A (TOKYO SHIBAURA ELECTRIC CO) 31 October 2001 (2001-10-31) column 3, line 2-13 column 3, line 49 -column 4, line 4 column 5, line 22-44 column 8, line 44 -column 9, line 51; claim 9 abstract	1-12,15, 17-28, 31,33
A	---	13,14, 29,30
X	US 6 308 273 B1 (SHAH BHARAT ET AL) 23 October 2001 (2001-10-23) column 1, line 43-52; claim 1 abstract	1,17,33
A	---	2-15, 18-31
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 November 2002	18. 12. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	MALIN SÖDERMAN /ELY

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internatk pplication No
PCT/IB 02/02045

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 084 968 A (HALL TIMOTHY GERARD ET AL) 4 July 2000 (2000-07-04) abstract ---	1-15, 17-31,33
A	DE 44 09 379 A (MOTOROLA AS) 22 September 1994 (1994-09-22) abstract -----	1-15, 17-31,33

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 02/02045

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [X] Claims Nos.: 16,32
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 16,32

The claims shall define the mattes for which protection is sought. Claims shall be clear and concise. They shall be fully supported by the description. Nor claims 16,32 or the description clearly describe the purpose for preventing the mobile device to enter a third/higher sequrity mode or how a more frequent input of identification or sequrity mode would prevent the mobile device from entering a third/higher sequrity mode.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatic .ppiication No
PCT/IB 02/02045

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1150531 A	31-10-2001	JP 2001312472 A	09-11-2001
		EP 1150531 A2	31-10-2001
		US 2001036273 A1	01-11-2001
US 6308273 B1	23-10-2001	EP 1095493 A1	02-05-2001
		JP 2002518720 T	25-06-2002
		WO 9965207 A1	16-12-1999
US 6084968 A	04-07-2000	NONE	
DE 4409379 A	22-09-1994	GB 2276287 A	21-09-1994
		DE 4409379 A1	22-09-1994